МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Идеалы полугрупп

ОТЧЁТ

ПО ДИСЦИПЛИНЕ

«ПРИКЛАДНАЯ УНИВЕРСАЛЬНАЯ АЛГЕБРА»

студентки 3 курса 331 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Шуликиной Анастасии Александровны

Преподаватель

профессор, д.ф.-м.н. ___________ В. А. Молчанов

подпись, дата

Саратов 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В данной лабораторной работе поставлена задача рассмотрения понятие идеалов полугрупп, разбор и реализация алгоритмов их построения, понятия и свойства отношений Грина на полугруппах, разбор и реализация алгоритмов вычисления отношений Грина и построения «egg-box»-картины конечной полугруппы.

1 Цель работы и порядок её выполнения

Цель работы – изучение строения полугрупп с помощью отношений Грина.

Порядок выполнения работы:

1. Рассмотреть понятия идеалов полугруппы. Разработать алгоритмы построения идеалов полугруппы по таблице Кэли.
2. Рассмотреть понятия и свойства отношений Грина на полугруппах.
3. Разработать алгоритмы вычисления отношений Грина и построения «egg-box»-картины конечной полугруппы.

2 Теория

2.1 Понятия идеалов полугрупп

Полугруппа – это алгебра $S = (S, \cdot)$ с одной ассоциативной бинарной операцией $\cdot$, т.е. выполняется $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ для любых $x, y, z \in S$.

Если полугрупповая операция называется умножением (соответственно, сложением), то полугруппу называют мультипликативной (соответственно, аддитивной).

Пусть S – произвольная полугруппа. Непустое подмножество $I \subset S$ называется правым (соответственно, левым) идеалом полугруппы S, если для любых $x \in I$, $y \in S$ выполняется условие: $xy \in I$ (соответственно $yx \in I$), т.е. $I \cdot S \subset I$(соответственно, $S \cdot I \subset I$). Если I – одновременно левый и правый идеал полугруппы S, то I называется двустронним идеалом (или просто идеалом) полугруппы S. Ясно, что в коммутативной полугруппе S все эти определения совпадают.

Лемма 1. Множество всех идеалов IdS(соответственно, левых идеалов $LIdS$ или правых идеалов $RIdS$) любой полугруппы S является системой замыкания.

Пусть X – подмножество полугруппы S. Тогда наименьший правый идеал полугруппы S, содержащий подмножество X, равен $(X] = XS^1 = X \cup XS$, наименьший левый идеал полугруппы S, содержащий подмножество X, равен $[X) = S^1X = X \cup SX$ наименьший идеал полугруппы S, содержащий подмножество X, равен $[X] = S^1XS^1 = X \cup XS \cup SX \cup SXS$.

В частности, любой элемент $a \in S$ определяет наименьшие правый, левый и двусторонний идеалы: $(a] = aS^1, [a) = S^1a$ и $[a] = S^1aS^1$, которые называются главными (соответственно, правыми, левыми и двусторонними) идеалами.

Минимальные относительно теоретико-множественного включения идеалы (соответственно, левые или правые идеалы) называются минимальными идеалами (соответственно, минимальными левыми или правыми идеалами).

Лемма 2. Если полугруппа имеет минимальный идеал, то он является ее наименьшим идеалом и называется ядром полугруппы.

Доказательство. Если I – минимальный идеал полугруппы S, то для любого идеала J полугруппы S непустое множество $IJ \subset I \cap J \subset I$ и, значит, идеал $I \cap J = I, I \subset J$.

Любая конечная полугруппа имеет наименьший идеал, т.е. ядро полугруппы.

Доказательство. Для конечной полугруппы S множество всех идеалов IdS конечно и, значит, его пересечение является наименьшим идеалом S.

2.1.1 Алгоритм построения идеалов полугруппы по таблице Кэли

Вход. Полугруппа S, таблица Кэли размерностью N, выполняющая свойство ассоциативности.

Выход. Множество правых идеалов R, множество левых идеалов L и множество двусторонних идеалов I.

Шаг 1. Строится множество res, состоящее из всех возможных комбинаций элементов полугруппы S (сочетание без повторений):$res = \{\{S_1\}, \{S_2\}, ..., \{S_N\}, ..., \{S_1, S_2\}, \{S_1, S_3\}, ..., \{S_1, S_N\}, ..., \{S_2, S_3\}, ..., \{S_2, S_N\}, ..., \{S_1, S_2, S_N\}\}$.

Шаг 2. Цикл i от 1 по N.

Шаг 2.1. Проверяем все подмножества множества res на выполнение условия правого идеала: если $\forall res_i \in res : xy \in res_i \forall x \in res_i, y \in S$, если условие выполняется, то res_i добавлем в множество R.

Шаг 2.2. Проверяем все подмножества множества res на выполнение условия левого идеала: если $\forall res_i \in res : yx \in res_i \forall x \in res_i, y \in S$, если условие выполняется, то res_i добавлем в множество L.

Шаг 2.3. Для того, чтобы множество res_i являлось двусторонним идеалом, оно должно удовлетворять условия правого и левого идеала. Если все подмножества множества res выполняют эти условия, то res_i добавляем в I.

Шаг 3. Выводится R, L, I.

Трудоемкость алгоритма $O(N^3 * M * M_2)$, M - размер множества res, M_2 - размер множества res_i.

2.2 Понятия и свойства отношений Грина на полугруппах

Отображения $f : a \mapsto [a]$, $f_r : a \mapsto (a]$, $f_l : a \mapsto [a)$, $a \in S$ определяют ядра $\mathscr{J} = kerf$, $\mathscr{R} = kerf_r$, $\mathscr{L} = kerf_l$ по формулам:

$$(a, b) \in \mathscr{J} \iff [a] = [b],$$

$$(a, b) \in \mathscr{R} \iff (a] = (b],$$

$$(a, b) \in \mathscr{L} \iff [a) = [b).$$

Все эти отношения, а также отношения $\mathscr{D} = \mathscr{R} \vee \mathscr{L}$, $\mathscr{H} = \mathscr{R} \cap \mathscr{L}$ являются эквивалентностями на множестве S, которые называются отношениями Грина полугруппы S. Классы этих эквивалентностей, порожденные элементом $a \in S$, обозначаются J_a, R_a, L_a, D_a и H_a, соответственно.

Лемма. Отношения Грина полугруппы S удовлетворяют следующим свойствам:

1. эквивалентность $\mathscr{R}$ регулярна слева и эквивалентность $\mathscr{L}$ регулярна справа, те. $(a, b) \in \mathscr{R} \Rightarrow (xa, xb) \in \mathscr{R}$ и $(a, b) \in \mathscr{L} \Rightarrow (ax, bx) \in \mathscr{L}$ для любых $x \in S$,
2. эквивалентности $\mathscr{R}$, $\mathscr{L}$ коммутируют,
3. $\mathscr{D} = \mathscr{R} \cdot \mathscr{L} = \mathscr{L} \cdot \mathscr{R}$,
4. если полугруппа S конечна, то $\mathscr{D} = \mathscr{J}$,
5. любой класс D эквивалентности $\mathscr{D}$ можно изобразить с помощью следующей egg-box-диаграммы, клетки которой являются классами эквивалентности $\mathscr{H}$, лежащими в D.

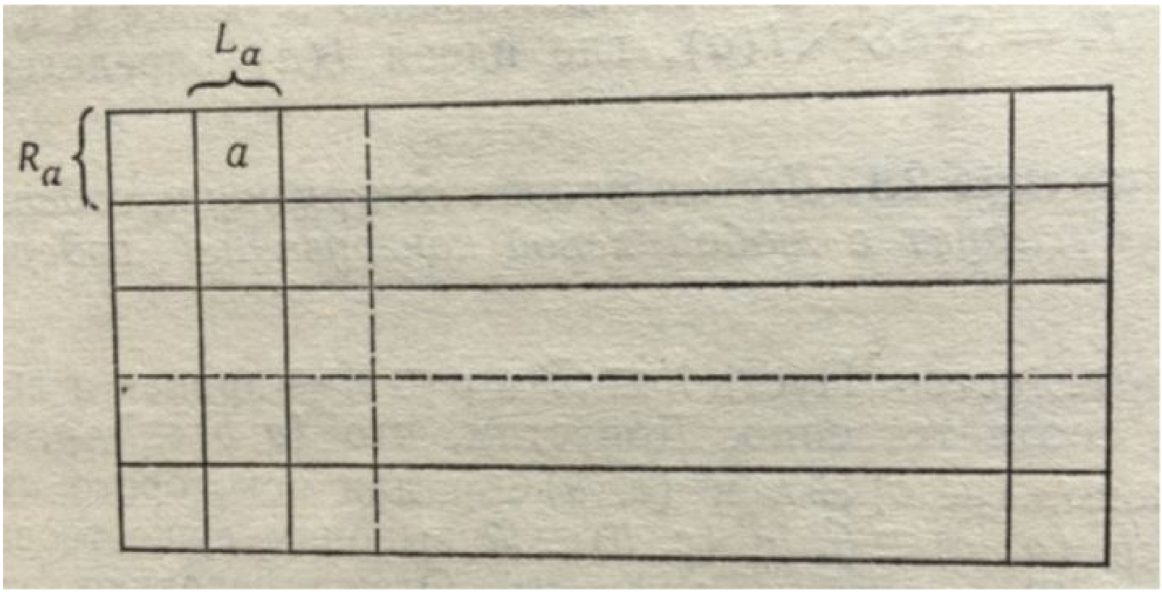


Рисунок 1 – egg-box-диаграмма

2.2.1 Алгоритм вычисления отношений Грина и построения «egg-box»-картины

Вход. Полугруппа S, таблица Кэли размерностью N, выполняющая свойство ассоциативности.

Выход. Отношения Грина $\mathscr{R}$, $\mathscr{L}$, $\mathscr{J}$, $\mathscr{H}$, $\mathscr{D}$ и «egg-box»-картины.

Шаг 1. Создаем булевую переменную $chek = true$.

Шаг 2. Цикл i от 1 до N.

Шаг 2.1. Для каждого i цикл j от 1 до N.

Шаг 2.2. $\forall S_i, S_j \in S$: строим правые идеалы $(S_i]$, $(S_j]$, если $(S_i] = (S_j]$, то добавляем (S_i, S_j) в множество $\mathscr{R}$.

Шаг 2.3. $\forall S_i, S_j \in S$: строим левые идеалы $[S_i)$, $[S_j)$, если $[S_i) = [S_j)$, то добавляем (S_i, S_j) в множество $\mathscr{L}$.

Шаг 2.4. $\forall S_i, S_j \in S$: строим двусторонние идеалы $[S_i]$, $[S_j]$, если $[S_i) = [S_j)$, то добавляем (S_i, S_j) в множество $\mathscr{J}$.

Шаг 2.5. Множество $\mathscr{H}$ строится: $\mathscr{H} = \mathscr{R} \cap \mathscr{L}$.

Шаг 2.6. Множество $\mathscr{D}$ строиться $\mathscr{D} = \mathscr{R} \cup \mathscr{L}$.

Шаг 3. Цикл по k от 0 до $D.size$.

Шаг 3.1. Проверяются все классы эквивалентности $\mathscr{R}$, если они совпадают с k-ым элментом множества $\mathscr{D}$, то они добавляются в $res1$.

Шаг 3.2. Проверяются все классы эквивалентности $\mathscr{L}$, если они совпадают с k-ым элментом множества $\mathscr{D}$, то они добавляются в $res2$.

Шаг 3.3. Цикл по i от 0 до $res1.size$, по j от 0 до $res2.size$, «egg-box»-картина строиться пересечением $res1_i$ и $res2_j$.

Шаг 4. Выводятся отношения Грина $\mathscr{R}$, $\mathscr{L}$, $\mathscr{J}$, $\mathscr{H}$, $\mathscr{D}$ и «egg-box»-картины.

Трудоемкость алгоритма $O(N^3)$.

2.3 Код программы, на основе рассмотренных алгоритмов, на языке C++

На рисунках 2-5 можно увидеть работу, реализуемой программы, по рассмотренным алгоритмам.

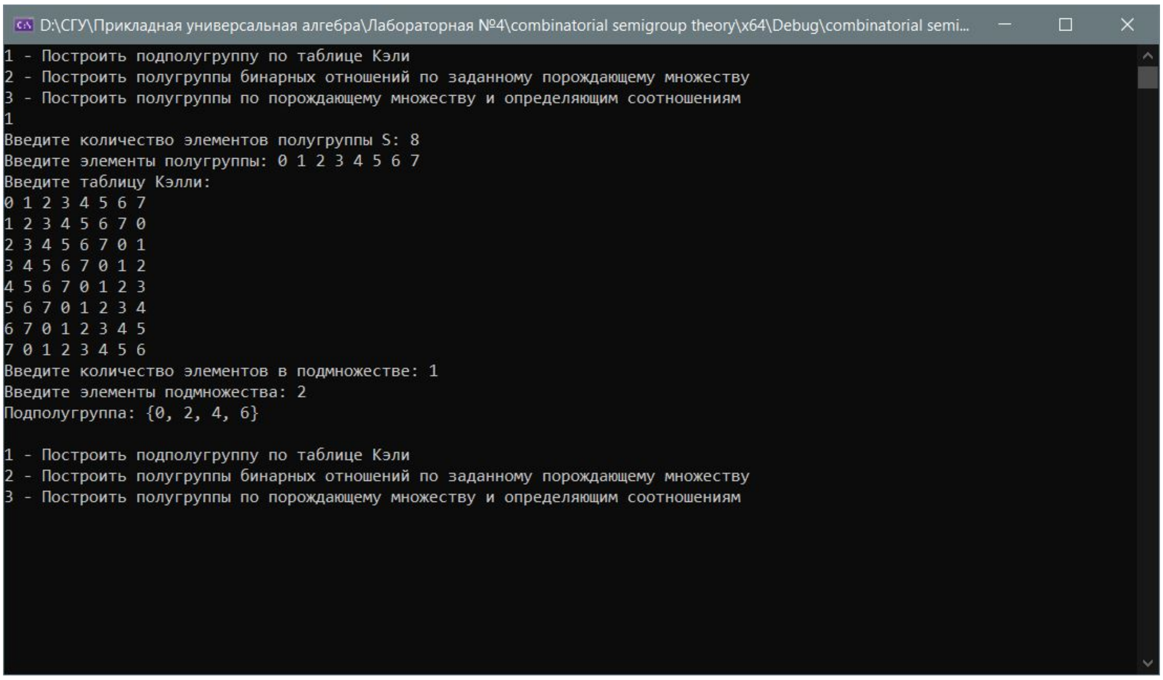
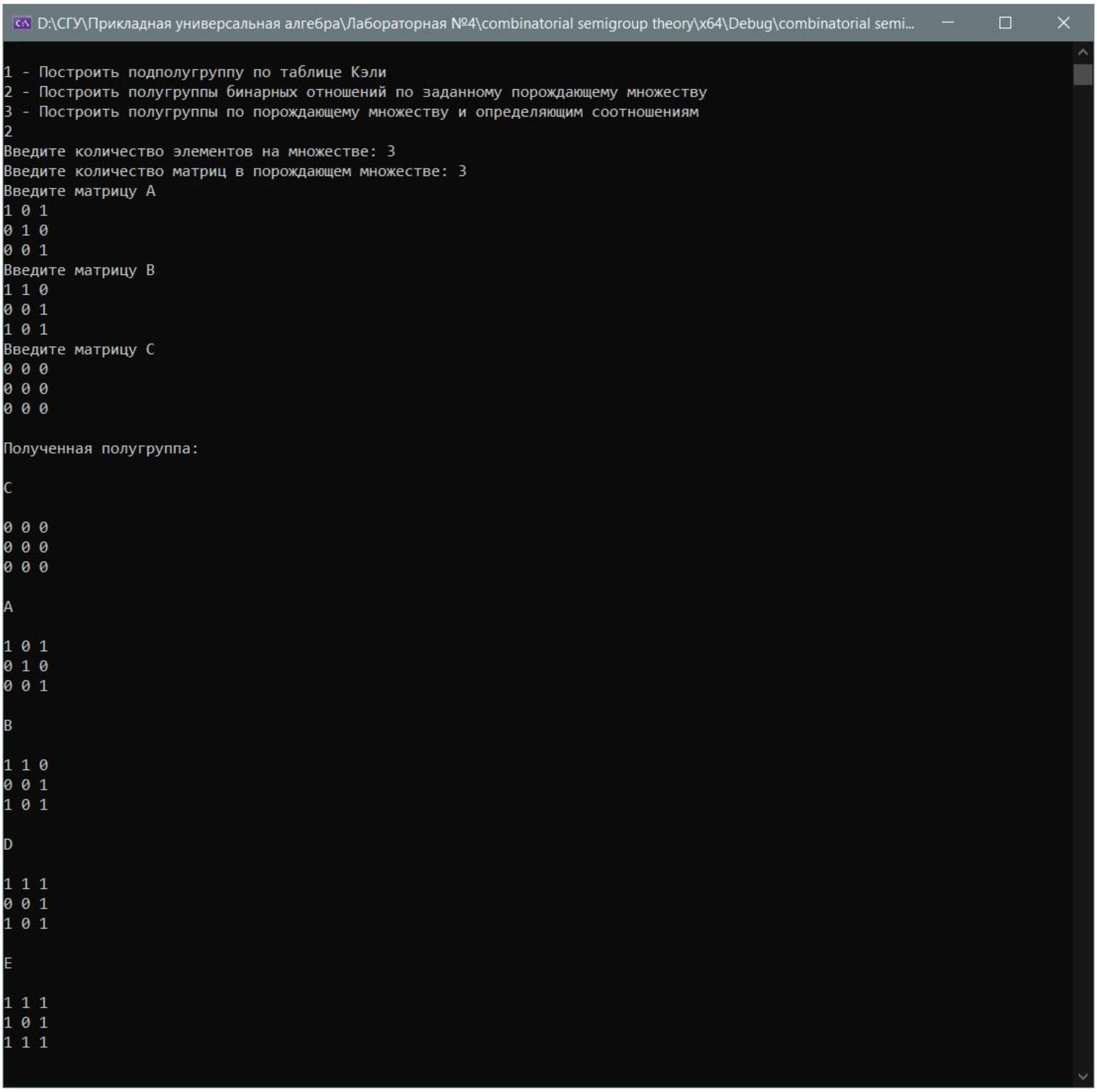


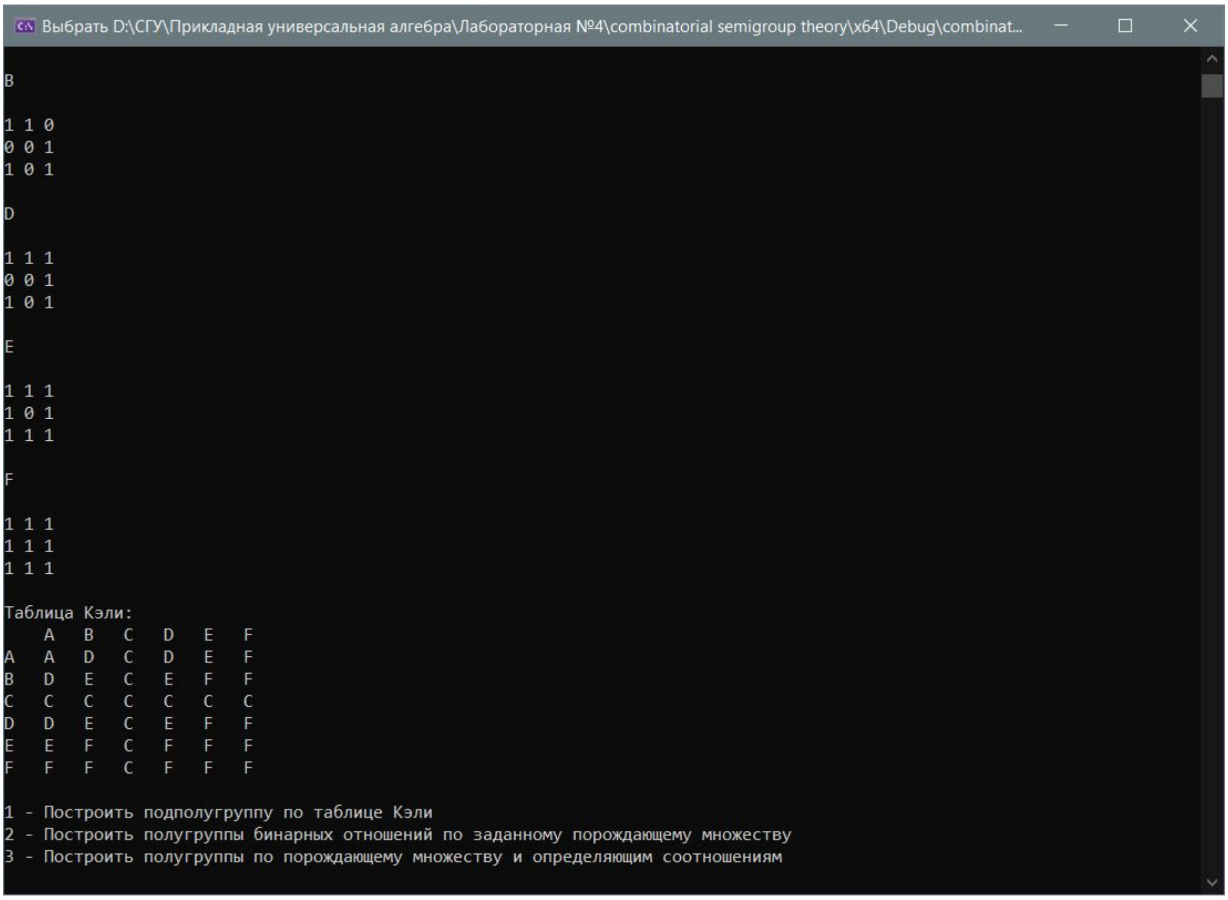
Рисунок 2



```
D:\СГУ\Прикладная универсальная алгебра\Лабораторная №4\combinatorial semigroup theory\x64\Debug\combinatorial semi...

1 - Построить подполугруппу по таблице Кэли
2 - Построить полугруппы бинарных отношений по заданному порождающему множеству
3 - Построить полугруппы по порождающему множеству и определяющим соотношениям
2
Введите количество элементов на множестве: 3
Введите количество матриц в порождающем множестве: 3
Введите матрицу A
1 0 1
0 1 0
0 0 1
Введите матрицу B
1 1 0
0 0 1
1 0 1
Введите матрицу C
0 0 0
0 0 0
0 0 0

Полученная полугруппа:

C

0 0 0
0 0 0
0 0 0

A

1 0 1
0 1 0
0 0 1

B

1 1 0
0 0 1
1 0 1

D

1 1 1
0 0 1
1 0 1

E

1 1 1
1 0 1
1 1 1
```

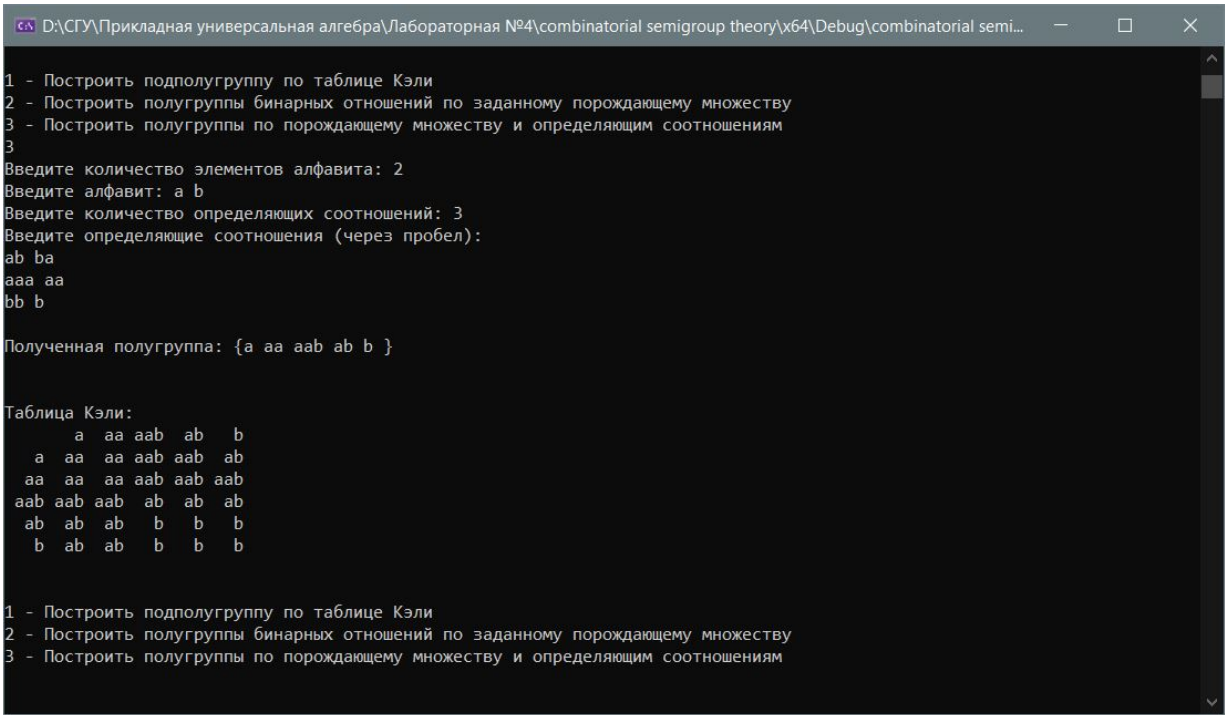
Рисунок 3

Листинг программы



```
Выбрать D:\СГУ\Прикладная универсальная алгебра\Лабораторная №4\combinatorial semigroup theory\x64\Debug\combinat...
B

1 1 0
0 0 1
1 0 1

D

1 1 1
0 0 1
1 0 1

E

1 1 1
1 0 1
1 1 1

F

1 1 1
1 1 1
1 1 1

Таблица Кэли:
    A   B   C   D   E   F
A   A   D   C   D   E   F
B   D   E   C   E   F   F
C   C   C   C   C   C   C
D   D   E   C   E   F   F
E   E   F   C   F   F   F
F   F   F   C   F   F   F

1 - Построить подполугруппу по таблице Кэли
2 - Построить полугруппы бинарных отношений по заданному порождающему множеству
3 - Построить полугруппы по порождающему множеству и определяющим соотношениям
```

Рисунок 4



```
D:\СГУ\Прикладная универсальная алгебра\Лабораторная №4\combinatorial semigroup theory\x64\Debug\combinatorial semi...
1 - Построить подполугруппу по таблице Кэли
2 - Построить полугруппы бинарных отношений по заданному порождающему множеству
3 - Построить полугруппы по порождающему множеству и определяющим соотношениям
3
Введите количество элементов алфавита: 2
Введите алфавит: a b
Введите количество определяющих соотношений: 3
Введите определяющие соотношения (через пробел):
ab ba
aaa aa
bb b

Полученная полугруппа: {a aa aab ab b }


Таблица Кэли:
       a   aa aab  ab   b
   a  aa   aa aab aab  ab
  aa  aa   aa aab aab aab
 aab aab aab  ab  ab  ab
  ab  ab   ab   b   b   b
   b  ab   ab   b   b   b


1 - Построить подполугруппу по таблице Кэли
2 - Построить полугруппы бинарных отношений по заданному порождающему множеству
3 - Построить полугруппы по порождающему множеству и определяющим соотношениям
```

Рисунок 5

ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы были рассмотрены понятия идеалов полугруппы, понятия и свойства отношений Грина на полугруппах, разобран алгоритм построения «egg-box»-картины конечной полугруппы. А также были реализованы алгоритм построения идеалов полугруппы по таблице Кэли, алгоритм вычисления отношений Грина и алгоритм построения «egg-box»-картины конечной полугруппы.